The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/

DATE ISSUED:
12/09/2016

SUBJECT:
A Vulnerability in Cisco IOS and IOS XE Software SSH X.509 Version 3 could allow for Authentication Bypass

ORIGINAL OVERVIEW:
A vulnerability in the implementation of X.509 Version 3 for SSH authentication functionality in Cisco IOS and IOS XE Software could allow an unauthenticated, remote attacker to bypass authentication on an affected system.

THREAT INTELLIGENCE:
There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- Cisco IOS
- Cisco IOS XE

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: N/A

TECHNICAL SUMMARY:
The vulnerability is due to improper validation of X.509 signatures during the SSH authentication phase. An attacker could exploit this vulnerability by presenting an invalid X.509 signature to an affected system. A successful exploit could allow the attacker to impersonate an existing valid user over an SSH connection.

RECOMMENDATIONS:
The following actions should be taken:

- Install updates once released by Cisco after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Administrators may disable the X.509 authentication feature on an affected device until the device is upgraded to a fixed release of the software.
- Unless required, limit external network access to affected products.

REFERENCES:
Cisco:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161207-ios-xe-x509

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6474

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.

http://www.us-cert.gov/tlp/